Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1807 02/19/16

~ Twitter ISIS Campaign! ~ People Are Talking! ~ Firebee Update News!
~ Hospital Pays A Ransom ~ Scary Red Gmail Symbol ~ Gmailify Your Mail!
~ 'Locky' Hijacks Systems ~ ~ 95% Share Passwords!

-* Coleco Chameleon Prototype! *-
-* Coleco Chameleon Package Information *-
-* New Outlook.com Premium Email Services Test *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Warm - cold! Snow - Rain! Blink, and the weather will change on you, if you’re living in New England. Yup, it’s been a strange winter so far. But, other than a few chilly shudders, you won’t hear me complaining! As of this date a year ago, we had about 95 inches of snow on the ground. This year, as of today, the snow cover is very patchy. I haven’t even fired up my snow thrower yet this winter! More snow and rain pedicted for this weekend, but temps in the 50’s are also on the way. I’ll live with it!

Speaking of "living with it," I’m not sure all of you [subscribers] have been receiving A-ONE in your mailboxes lately. I haven’t, but I just thought it might be a glitch on my end. But, a couple of others mentioned similar problems; and, I noticed a note on usenet mentioning that, among other site, the A-ONE site was "missing." So, I’m looking into the possibility that there may be may be a problem with our site which would result in failed e-mails via our domain. Meanwhile, I hope that you’ve found recent issues via our other outlets.

Following U.S. presidential politics? What a 3-ring circus out there! Personally, I’m really tired of the politics-as-usual and I’ve lost a lot of trust in our national government. It’s really time for a major shake-up or change, but I don’t know if this country is ready for it. While I don’t know if I’d vote for a Donald Trump or Bernie Sanders, I have to admit that I like a lot of what they have to say. And it’s true, there’s some that makes me want to cringe! But, there’s even more going on from the "mainstream" group of politicians that also makes me cringe even more! It’s going to be a very interesting election year!

Sorry for a smaller-than-usual issue this week. I was considering delaying this issue a week due to the amount of articles, but I decided that I didn’t want to get into a habit of missing issues too often. We were "short" but bearable this week. Hopefully the news will pick up again quickly.

Until next time...

=~=~=~=

FireBee Update News

By Fred Horvat

As stated in past submissions I was having problems with the FireBee not always booting properly or doing other strange things while booting. A small number of FireBee owners started having this issue after we upgraded our BaS (BasicSystem) Firmware. The solution is to reflash the BaS to the original CodeWarrior Version located here: http://firebee.org/~firebee/pictures/files/BaS-20120613.zip.

Well I finally did get around to reflashing the FireBee with the original BaS Firmware. Since then the FireBee has booted up fine the couple of times that I have used it since reflashing the firmware. Someone contacted me on http://atari-forum.com/ about a newer BaS upgrade but for now since the FireBee appears to be working properly I am going to leave it as is.

=~=~=~=

->In This Week's Gaming Section - Coleco Chameleon Prototype Shown at New York Toy Fair!
"""""""""""""""""""""""""""""""" Coleco Chameleon Package Information!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Coleco Chameleon Prototype Shown at Closed to Public New York Toy Fair

The RETRO Video Game Systems team has been on a roller coaster ride since the very first announcement of their intent to launch a console. Formerly known as the RETRO Video Game System, now after acquiring a license to use the name Coleco they have renamed it the Coleco Chameleon. Earlier today, at the New York Toy Fair the RVGS Inc founder/mouthpiece/PR/marketing executive, Mike Kennedy, showed a little bit of gameplay for the Coleco Chameleon in a heavily edited video. Some interesting things are shown and now available for analyzation by the public.

What is shown in the video is hardwired into the prototype Super Nintendo controllers. According to their Facebook page, the

controllers they will be using as the official Coleco Chameleon controllers contain many options (Analog sticks) [which] aren t working with these games at this time. This is understandable as this is a prototype and not the final hardware. I do think it is poignant to point out that the official controllers do include all of the buttons that the SNES controller does so it is glaring that those are not being used here.

As many on AtariAge/comments on the Chameleon video on FB have pointed out there is no power going to the LED on the console. Considering this is a prototype that is probably to be expected. According to RETRO Video Game Systems Inc comments regarding this issue, the console powers on when plugged in- obviously this will change before the unit is put into production.

For anyone interested in that cartridge, it has Coleco Chameleon Prototype 1 printed on a white sticker.

So, has this made you a believer in the Coleco Chameleon? Will you be getting one? It is rumored that these won t be hitting Kickstarter backers till sometime in 2017 (with a Kickstarter starting in less than two weeks). Is that a damper? It would give developers proper time to get games ready (games don t just click together and work).

Coleco Chameleon To Package Custom USB Controllers With ColecoVision and Intellivision Compilation Carts

The Coleco Chameleon will apparently be releasing ColecoVision and Intellivision compilation carts with custom USB controllers. This answers a question that many have had about the future of this platform. Supporting ColecoVision and Intellivision games has been repeatedly mentioned by the management team of the Chameleon. Apparently, early on only compilation carts for ColecoVision and Intellivision games will be made available. The inclusion of custom USB controllers for each console will alleviate concerns of fans as to how multi button games will be played on the Coleco Chameleon.

Mike Kennedy, founder of RETRO Video Game Systems Inc who are launching the Coleco Chameleon, stated that in the future they may release adapters. Mention of the adapters was centered on the ColecoVision and Intellivision games of yesteryear. In an interview with me here at Retro Gaming Magazine, Mike Kennedy and his, then, team were confident in releasing adapters for many different platforms. There was no mention of these other adapters in the short interview done with SEO Toy Review on Youtube.

Presumably the controllers for ColecoVision and Intellivision will be made available separately. This is ideal if there is to be more than one compilation release for each of these classic consoles. This does raise the problem of having two skews for stores to stock- one with the custom controller and one without it (for those that own a previous compilation).

Also there is no word on whether only one controller will be

included or if each compilation release will feature two controllers (for the many two player games on each console).

Considering the controller that RETRO Video Game Systems plans on including with the Coleco Chameleon I wonder if they will offer compilations for other platforms with USB controllers too? From the NES to the Genesis, button layouts are usually unique to each console. The pack-in controller is only ideal for Playstation and Super Nintendo gaming. Consoles such as the Turbo Grafx-16, Sega Genesis, NES, Atari 2600, etc (all mentioned as seeing potential support previously) have unique button layouts that simply don t fit the pack-in controller.

The Coleco Chameleon is currently on display at the New York Toy Fair, as covered here on RGM.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Twitter s Account Suspensions Are Surprisingly Effective Against ISIS

Plagued with complaints from lawmakers and officials that it s too soft on Islamic State terrorists and their online supporters, Twitter has stepped up the pace and breadth of account suspensions during the past year. And according to new research, its campaign to curb the group s propaganda reach seems to be working.

According to J.M. Berger and Heather Perez, Twitter s routine pruning of Islamic State-associated accounts has kept the size of the Islamic State s propaganda network small, and has particularly damaged the reach and influence of the largest and most prominent accounts.

The researchers findings, published Thursday by the George Washington University s Program on Extremism, temper a general sense of panic among government officials, sparked by the impression that the Islamic State is winning a propaganda war against the Western world.

Top lawmakers have lamented the effectiveness of the group s grassroots-like Twitter apparatus, and have launched shaky attempts to counter it. In doing so, they have painted a picture of a well-oiled propaganda machine that floods Twitter, Facebook, and Telegram with pro-jihadi messages that inspire Westerners to either travel to Iraq and Syria, or commit acts of terrorism at home.

Indeed, Islamic State-affiliated accounts have spread violent images, propaganda videos, and calls to action online. But their

influence is waning.

Berger and Perez determined that there s usually an average of only 1,000 easily discoverable English-speaking terrorist accounts at a time, and that the average Islamic State supporter has only 300 to 400 followers. And those accounts appear to be stuck in an echo chamber: They generally only interact with other supporters, rather than spreading their message to new followers.

The researchers monitored a list of ISIS supporters accounts maintained by hand by a particularly active supporter for a period of nearly four months in 2015, making note of account suspensions and new additions to the list.

At times, Twitter suspended the list members accounts at a high pace, sometimes even suspending a user multiple times in one day. But most of the time, only about 2 percent of the list was suspended every day.

Berger has long railed against the whack-a-mole thesis of Twitter takedowns the idea that suspending an online account is a waste of time because new accounts will quickly sprout up to take the place of a deleted one. To test that theory, he and Perez tracked four users as they were repeatedly suspended by Twitter and reemerged every time with a different name.

We found suspensions typically had a very significant detrimental effect on these repeat offenders, shrinking both the size of their networks and the pace of their activity, the researchers wrote. Returning accounts rarely reached their previous heights, even when the pressure of suspension was removed.

Twitter has further accelerated the pace of its account removals in the months after the researchers study period. Just a few weeks ago, the company announced that it has taken down 125,000 terrorist-related accounts since mid-2015. The company also said that staffing increases had led to quicker takedowns.

But a few lawmakers have repeatedly pushed for legislation that would require social-media companies like Twitter and Facebook to do more. A bill from Richard Burr and Dianne Feinstein, the chairman and vice-chair of the Senate Intelligence Committee, would require the platforms to report terrorist activity on their networks to law enforcement. But concerns about freedom-of-speech violations and the potential loss of valuable intelligence from terrorists on Twitter has led opponents in and out of the Senate to speak out against the proposal.

If Twitter can show that its own increasingly aggressive campaigns to stomp out propaganda are working, perhaps it can dodge a legislative intervention one that would burden social-media companies with heavy reporting duties and bring another platform under government surveillance.

California Hospital Makes Rare Admission of Hack, Ransom Payment

While it was not the first hacked organization to acquiesce to attackers' demands, the California hospital that paid $17,000 in ransom to hackers to regain control of its computer system was unusual in one notable way: It went public with the news.

Hollywood Presbyterian Medical Center relented to the demands, President Allen Stefanek said, because he believed it was the "quickest and most efficient way" to free the Los Angeles hospital's network, which was paralyzed for about 10 days.

That announcement sparked fears Thursday among hospitals and security experts that it would embolden hackers to launch more "ransomware" attacks and calls in California for tougher laws.

It s no different than if they took all the patients and held them in one room at gunpoint, said California State Senator Robert Hertzberg, who on Thursday introduced legislation to make a ransomware attack equivalent to extortion and punishable by up to four years in prison.

Usually embarrassment and a desire to discourage hackers keep attacked companies quiet. Hollywood Presbyterian did not say why it made the disclosure, but its hand may have been forced by spreading rumors a week after the hack. Stefanek confirmed the cyber attack after at least one doctor appeared to have told local media.

In addition, he disputed media reports the 434-bed hospital had faced a ransom demand of $3.4 million, far more than the amount paid in the hard-to-trace cyber-currency bitcoin.

In a ransomware attack, hackers infect PCs with malicious software that encrypts valuable files so they are inaccessible, then offer to unlock the data only if the victim pays a ransom.

The hack at Hollywood Presbyterian forced doctors to use pen and paper in an age of computerization. News reports said its fax lines were jammed because normal e-mail communication was unavailable, and some emergency patients had to be diverted to other hospitals.

Investigators said administrators were so alarmed that they may have paid ransom first and called police later.

Medical facilities in the area plan to consult cyber security experts on how to protect themselves, the Hospital Association of Southern California said. Hospitals are certainly now aware of ransomware more than they ever were before, and this has become a very real threat, said spokeswoman Jennifer Bayer.

Some experts said ransomware encryption can be so hard to crack that victims feel they have little choice but to pay if they want their systems back. The hackers' success could also prompt other hospitals to make quick payments to avoid the disruption and bad publicity Hollywood Presbyterian faced.

Our number one fear is that this now pretty much opens the door for other people to pay," said Bob Shaker, a manager at cyber security firm Symantec Corp.

He knew of at least 20 other attacks on healthcare facilities in the past year and hundreds more in other industries that had been kept secret.

Some of those put patients at risk and affected infusion pumps that deliver chemotherapy drugs, risking patient overdoses, he said.

Because hackers hide their identities and demand payment in bitcoin, authorities may have to work harder to find them than if they used old-fashioned methods.

But cyber-crime experts say that they can still be traced.

"The public nature of the network does give law enforcement an angle to help defeat them," said Jonathan Levin, co-founder of Chainalysis, a New York company working with bitcoin users. "But it s a game of cat and mouse."

Ransomware is big business for cyber criminals and security professionals. Although ransoms typically are less than the hospital paid, $200 to $10,000, victims of a ransomware known as CryptoWall reported losses over $18 million from April 2014 to June 2015, the FBI said.

Ransomware attacks climbed sharply in 2014, when Symantec observed some 8.8 million cases, more than double the previous year. IBM said that last year more than half of all customer calls reporting cyber attacks involved ransomware.

How Just Opening An MS Word Doc Can Hijack Every File On Your System

If you receive a mail masquerading as a company’s invoice and containing a Microsoft Word file, think twice before clicking on it.

Doing so could cripple your system and could lead to a catastrophic destruction.

Hackers are believed to be carrying out social engineering hoaxes by adopting eye-catching subjects in the spam emails and compromised websites to lure the victims into installing a deadly ransomware, dubbed "Locky," into their systems.

So if you find .locky extension files on your network shares, Congratulations! You are infected and left with just two solutions: Rebuild your PC from scratch or Pay the ransom.

Locky ransomware is spreading at the rate of 4000 new infections per hour, which means approximately 100,000 new infections per day.

It is hard to digest the fact that, in this 2016, even a single MS Word document could compromise your system by enabling ’Macros.’

This is where the point to appreciate hacker’s sheer brilliance

of tactics.

Locky ransomware is being distributed via Microsoft 365 or Outlook in the form of an Invoice email attachment (Word File that embeds vicious macro functions).

The concept of macros dates back to 1990s. You must be familiar with this message: "Warning: This document contains macros."

Now macros are back, as cyber criminals discover a new way to get internet users to open Microsoft Office documents, especially Word files that allow macros to run automatically.

Once a user opens a malicious Word document, the doc file gets downloaded to its system. However, danger comes in when the user opens the file and found the content scrambled and a popup that states "enable macros".

Here comes the bad part:

> Once the victim enables the macro (malicious), he/she would download an executable from a remote server and run it. This executable is nothing but the Locky Ransomware that, when started, will begin to encrypt all the files on your computer as well as network.

Locky ransomware affects nearly all file formats and encrypts all the files and replace the filename with .locky extension.

Once encrypted, the ransomware malware displays a message that instructs infected victims to download TOR and visit the attacker’s website for further instructions and payments.

Locky ransomware asks victims to pay between 0.5 and 2 Bitcoins ($208 to $800) in order to get the decryption key.

One of the interesting note on Locky is that it is being translated into many languages, which heighten its attack beyond English boundaries to maximize the digital casualties.

The new ransomware also has the capability to encrypt your network-based backup files. So it’s time for you to keep you sensitive and important files in a third party storage as a backup plan in order to evade future-ransomware infections.

A researcher named Kevin Beaumont along with Larry Abrahms of BleepingComputer initially discovered the existence of Locky encrypted virus.

To check the impact of Locky, Kevin successfully intercepted the Locky traffic yesterday and realized that the cryptovirus is spreading out rapidly in the wild.

"I estimate by the end of the day well over 100,000 new endpoints will be infected with Locky, making this a genuine major cybersecurity incident 3 days in, approximately a quarter of Million PCs will be infected," Kevin said in a blog post.

What That Scary New Red Gmail Unlocked Symbol Means

In recent days, some Gmail users have been wondering and worrying about new emails popping up in their inboxes with a new unlocked icon.

Have no fear. As we mentioned on Tuesday, this is just Google s way of telling you that an email you ve received isn t as secure as it should be.

Emails that have not been authenticated by TLS encryption (transport layer security) will show this red unlocked icon, but that doesn t necessarily mean that the sender is an evil spammer sneaking into your inbox.

What TLS encryption does is protect the security of email messages as they travel from sender to recipient. That encryption makes sure that the sender s email remains private, preventing third parties from taking a peek at the message or tampering with it as it makes its way to its final destination.

So if you see this icon, and the message has anything to do with sensitive information (finances, passwords, etc.), you should be concerned and take steps to contact the sender about the insecure email. But outside of emails containing sensitive information, that scary lock icon may just be an indication that the email could be compromised or that sender isn t taking its security as seriously as they should be.

Again, if you see the red unlocked icon, don t immediately reach for the Send to Spam button, just take special note of that particular message. No need to panic, just keep your guard up.

Gmailify Offers The ’Best of Gmail’ Without A Gmail Address

Get "all the bells and whistles" of Gmail without ditching your current email address.

Attached to a certain email address that doesn’t end in @gmail.com, but want Gmail features like spam protection and better inbox organization? Now you can have it all.

Google on Wednesday introduced a new tool called Gmailify, which lets you link an existing Microsoft Outlook, Hotmail, or Yahoo! Mail account to Gmail so you get "all the bells and whistles" of Google’s email service without ditching your current address. Those perks include Google’s advanced spam detection and blocking, a tabbed inbox that organizes your mail into groups, and Google Now cards that call out things like travel and hotel reservations based on your mail.

If you’re already accessing your third-party email from the Gmail Android app, you’ll just need to enable the "Gmailify" feature and you’re good to go. If you don’t already have a Gmail account, you’ll need to first set one up to try this out; head over to

Google’s Support page for more detailed instructions.

Once you get it set up, when you sign in to the linked Gmail address you’ll see your messages from the other provider in your mailbox, and you’ll be able to read, reply, and organize your external mail just like you do in Gmail.

"Of course, you’re always in control so if you ever change your mind, you can unlink your account(s) at any time, and continue to access them through the Gmail app without using Gmailify," Google Software Engineer Michael Käser wrote in a blog post. "We’re really excited to bring the best of Gmail to more people, and we’re planning to add other email providers to Gmailify in the future."

Google first rolled out its tabbed Gmail inbox in 2013. The feature groups your mail into categories that you can pick, like Social, Promotions, and Updates alongside Primary, which is reserved for your most important messages.

95% of Americans Share Passwords With Friends and Family Members

Online security has been one of the hottest topics on the planet for the past several years. Between Edward Snowden, the Sony hack, the Target hack and Hillary Clinton s private email server, you would think that Americans would be on top of their own personal security when it comes to online accounts that contain sensitive information.

Unfortunately, you d be mistaken.

According to the results a recent survey from the developers behind password management app LastPass, 95% of Americans share between one and six passwords with friends or family members. This is in spite of the fact that 73% of them admit that they are taking a risk by doing so.

You might think that you re not one of the millions sharing passwords, but if you ve ever given anyone your Wi-Fi password or allowed someone to log in to your Netflix or HBO account, you re a member of this massive group.

 Nearly all aspects of our lives have some online component and when you bring password sharing into the mix, all of that sensitive information is instantly compromised, said LastPass Vice President Joe Siegrist.

Although letting a trusted friend jump on your Wi-Fi network might not be all that risky, another statistic from the survey is far more worrisome. Security experts will tell you that repeating passwords is one of the biggest mistakes you can make, but 59% of the 1,053 people surveyed said they reuse passwords on multiple sites.

If your Netflix password happens to be the same as your bank account password, an innocuous decision to share with a careless friend could suddenly leave you thousands of dollars in the hole.

So, for the last time: use a password manager.

Microsoft Testing New Outlook.com Premium Email Service

Microsoft is piloting a new version of its Outlook.com email, known as Outlook.com Premium.

Outlook.com Premium seems to be different from the current ad-free Outlook.com service that Microsoft currently sells for $19.95 per year. Ad-free Outlook.com, the successor to Hotmail Plus, removes graphical ads; no need to log in to keep an account active; and free technical support.

Microsoft isn't talking about when and whether the company plans to roll out Outlook.com Premium or how much (if anything) it will cost to subscribe.

But one of the features to which Outlook.com Premium testers have access is the ability to set up new custom domain accounts. Microsoft began winding down custom domain support in Outlook.com in 2014. While existing Outlook.com custom-domain holders were able to retain existing custom email addresses, Microsoft stopped accepting new registrations for the service and no longer allowed those with custom email addresses to add or remove addresses.

A Microsoft spokesperson confirmed that the company is piloting Outlook.com Premium and evaluating the return of a modified custom domain service.

"Outlook.com Premium is not an existing offering, it is an experiment that we are piloting. We're always investigating new features based on the wants and needs of our users, and we have nothing more to share at this time," the spokesperson told me after I asked about this Web page, brought to my attention by a reader.

On the custom domain front, the spokesperson said:

> "We are evaluating interest in custom domains for Outlook.com. At this time, we are testing with a limited number of users in the United States and will evaluate the experience over time. The previous program required the user to manage the process of purchasing a domain. We are evaluating the appeal of custom domains but with Microsoft managing the processes of procuring the domain."

In other Outlook.com news this week, Microsoft removed the "preview" tag from its updated Outlook.com experience, but still has yet to roll out the updated service to many.

Microsoft officials said in May 2015 that they'd be updating Outlook.com with new features that would make it look and feel more like "real" Outlook. The plan was to bring Outlook and Outlook.com closer together so that users feel like there are fewer differences between these two different email products that are both called "Outlook." The move was similar to what the

company is doing in terms of bringing together Skype and Skype for Business (Lync), and OneDrive and OneDrive for Business.

Users of Microsoft's Outlook.com email service can now make and receive Skype calls directly from their inbox.

In August 2015, Microsoft expanded the very limited number of users who had received the new Outlook.com preview. As of Febraury 2016, Microsoft is continuing to roll out the updated service worldwide. Microsoft officials said this week that they are rolling out the new experience "to millions of users each week."

Brand-new Outlook.com users get the new version of Outlook.com upon sign up in North America and in the coming weeks in other parts of the world. Existing Outlook.com users: Microsoft still is saying we'll get the updated version of the service "soon." Existing Outlook.com users don't need to do anything; settings and data will be automatically transferred. Users' Outlook.com email addresses will remain the same.

I asked Microsoft if existing Outlook.com users can opt out or are able to get a heads-up before they are transferred. I believe the answer on both of these is no, but I still have yet to hear back.

As Microsoft officials said last May, the updated Outlook.com is "powered by Office 365," which means it will share some of the same platform-level components - though not actually use Exchange on the back-end like Outlook does.

The new Outlook.com also will include not just features announced in May 2015, but also add-ins announced late last year, such as suggested contacts and automatic flight notifications. Add-ins for Uber, PayPal, Evernote, Wunderlist and other apps are also going to be part of the new experience, as announced last August.

=~=~=~=